ntdll.dll symbols are missing?

Posted by noname - 23 Nov 2011 - 04:05

Hi all.

I have a problem with ntdll.dll symbols. Actually, I just have no .pdb files for it, however all of pdb's are downloaded from microsoft site (I use symbol server for windbg, actually). And when I try to debug in kernel mode I've got troubles of course, that's not surprising - !peb and other stuff like !object or dt nt !PEB doesn't work too.

PDF created: 18 Jun 2025, 23:58

Can anyone suggest an issue?

Re: ntdll.dll symbols are missing? Posted by noname - 23 Nov 2011 - 10:25

Oh... I've already solved the problem with windbg - I just downloaded local symbols and then gave them to symstore. It's okay now, but !peb doesn't work, neither dt PEB or dt nt! PEB, however lml shows that ntdll.pdb has been loaded. I debug XP SP3 so the symbols do fit the system.

kd>!peb 7ffdb000 PEB at 7ffdb000 error 1 InitTypeRead(nt! PEB at 7ffdb000)...

However this value is the right one - I've taken it from Peb field of !process 0 0 output.

kd> dt _PEB 7ffdb000

ntdll! PEB

+0x000 InheritedAddressSpace: ?? +0x001 ReadImageFileExecOptions: ??

+0x002 BeingDebugged : ?? +0x003 SpareBool : ?? +0x004 Mutant : ????

+0x008 ImageBaseAddress: ????

: ???? +0x00c Ldr

+0x010 ProcessParameters: ???? +0x014 SubSystemData : ???? +0x018 ProcessHeap

//and so on

I'm really at a loss;